UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 11-60285-CR-ROSENBAUM

UNITED STATES OF AMERICA,

Plaintiff,

vs.

DARYL DAVIS and
HASAM WILLIAMS, et al.,

Defendants.
_____/

GOVERNMENT'S RESPONSE TO THE COURT'S ORDER AND MOTION FOR A PROTECTIVE ORDER PURSUANT TO SECTION 4 OF THE CLASSIFIED INFORMATION PROCEDURES ACT AND RULE 16(d)(1) OF THE FEDERAL RULES OF CRIMINAL PROCEDURE AND MEMORANDUM OF LAW

REDACTED, UNCLASSIFIED VERSION

I. INTRODUCTION

The Government is filing this Response, Motion and Memorandum of Law, *ex parte*, *in camera*, and under seal, in response to the Court's June 10, 2013 Order Requiring Response from Government, and in support of its Motion for a Protective Order Pursuant to Section 4 of the Classified Information Procedures Act ("CIPA"), 18 U.S.C. App. 3, and Fed. R. Crim. P. 16(d)(1).[1] This response and motion concerns

[1] The government is filing this pleading and supporting materials *ex parte*, *in camera,* and under seal with the Classified Information Security Officer or his designee because an adversarial or public proceeding would result in the unauthorized disclosure of classified information. As discussed at greater length at Section III.B.2, *infra*, an *ex parte*, *in camera* procedure is appropriate under CIPA to protect classified information. *See, e.g.*, *United States v. O'Hara*, 301 F.3d 563, 568 (7th Cir. 2002) (district court properly conducted *in camera*, *ex parte* proceeding to determine whether classified information was discoverable); *see also United States v. Campa*, 529 F.3d 980, 994-95 (11th Cir. 2008) (district court did not abuse its discretion by holding an *ex*

certain classified information, which Defendant Terrance Brown argues is related to this prosecution, and which he believes to be in the United States Intelligence Community's possession, based on unauthorized disclosures of classified information to the press.[2]

[CLASSIFIED INFORMATION REDACTED][3]

In his motion, the defendant primarily seeks to compel production of cell site locational data, i.e. information about where a cellular telephone was geographically located at the time a call was made ("CSLI"), during July 2010 for Metro PCS cellular telephone number (786) 307-4240,[4] based on public reporting about the collection of call data records under a classified order by the Foreign Intelligence Surveillance Court ("FISC"). The information acquired under this program, however, did not include CSLI. Thus, the government does not possess the records the defendant seeks.

[CLASSIFIED INFORMATION REDACTED]

For these reasons, the Government hereby requests that this Court, pursuant to CIPA Section 4 and Rule 16(d)(l): (1) conduct an *in camera* and *ex parte* review of the Government's submission; (2) deny the Defendant's Motion to Compel Production of Phone Records and request for a Rule 17 subpoena to obtain the records, because the Government has no reason to believe that responsive records exist under *Brady v. Maryland*, 373 U.S. 83 (1963), and Fed. R. Crim. P. 16; (3) find that to the extent any

---

parte hearing under CIPA Section 4). Rule 16 similarly contemplates *ex parte*, *in camera* proceedings, on a showing of good cause. *United States v. Hamaker*, 455 F.3d 1316, 1328 (11th Cir. 2006) (citing Fed. R. Crim. P. 16(d)(1)).

[2] [CLASSIFIED INFORMATION REDACTED]

[3] As a result of the redactions, the pagination and footnote numbering of the classified pleading and the unclassified version are different.

[4] Initially, the Defendant asked for records for Metro PCS cellular telephone numbers, (786) 307-4240 and (786) 419-2326, but in a June 18, 2013 hearing, he withdrew his request for information about the second number.

records existed, they should be deleted from discovery under CIPA Section 4; (4) strike the Defendant's Notice under CIPA Section 5; and (5) order that the entire text of this motion, all accompanying exhibits and any classified order issued by the Court shall not be disclosed to the defendants and shall be sealed and preserved in the records of the Court to be made available to the appellate court in the event of an appeal. The Government is requesting this order because the disclosure of the classified material could be reasonably expected to cause exceptionally grave damage to the national security of the United States.

A. Background

1. The Criminal Case and Defendant's Motion

As the Court is aware, Terrance Brown and his co-defendants are charged with multiple felonies relating to two attempted robberies of Brink's Security employees, and felony murder with a robbery on October 1, 2010, during which a Brink's security guard was killed. The government also advised the defendants of its intent to present as evidence cell phone records (including CSLI) obtained by the government and turned over in discovery for phones belonging or linked to the defendants (DE 213, 300, 441, 649); and expert testimony referencing charts and maps regarding the cell site information (DE 590). The parties vigorously litigated the admissibility of the cell site evidence (DE 453, 467, 471, 472, 476, 477, 502, 503, 504, 506, 559 [cell site evidence]; DE 590, 595, 604, 605, 613, 664, 677, 682, 700 [expert testimony and exhibits regarding cell site records]).

On May 24, 2013, Brown and his co-defendants proceeded to trial (DE 742). As part of its evidence linking the defendants to the charged offenses, the government

presented substantial testimony and records regarding the activity of cell phone numbers linked to Brown and his co-defendants during the time period relevant to the attempted robberies on July 26, 2010 (Counts 2-3) and September 17, 2010 (Counts 4-5), and the robbery and murder on October 1, 2010 (Counts 6-8). Specifically, the government used cellular tower data to determine the location of certain telephones associated with the defendants, including Brown, to demonstrate where they were during the crimes charged and other relevant dates. Although the government obtained cell phone records for numbers/phones linked to several of Brown's co-defendant for July, 2010 and September 1, 2010 to October 19, 2010, the government was unable to obtain cell phone records for Brown, (786) 419-2326 and (786) 307-4240, ("Brown's cell phone numbers") for dates prior to September 1, 2010, because the cell phone carrier – Metro PCS – no longer had the records by the time it received the government's subpoena. At trial, the government used records obtained from one co-defendant's cell phone on July 10, 2010 (DE 778, at 1), July 12, 2010 (DE 778, at 2), July 19, 2010 (DE 778, at 3), and July 21, 2010 (DE 778, at 4), as evidence linking Brown to the charged offenses. There was no cell phone activity linked to Brown on July 26, 2010 (DE 778, at 5).

On June 9, 2013, Brown filed a Motion to Compel Production of Phone Records for Brown's cell phone numbers for July 2010 (DE 778). Brown argues that although the government was previously unable to provide those records because Metro PCS had deleted them before receiving the government's subpoena, it now appears likely that the National Security Agency ("NSA") has those records (DE 778, at 2-3). In support of his argument, Brown relies on a June 5, 2013, article published in the *Guardian* newspaper discussing a classified Foreign Intelligence Surveillance Act ("FISA") order directing

Verizon to provide cell phone data – including cell phone location data – to the NSA. While Brown acknowledges that the classified order involves Verizon, not Metro PCS, he argues that comments by President Obama and members of Congress about the classified order and a related program entitled PRISM, show that the NSA has been collecting cell phone information from all cell phone providers, not just Verizon, since 2006 (*id*).

Brown, who has neither challenged the government's evidence linking him to the (786) 307-4240 cell phone number nor stipulated to ownership of the phone,[5] contends that the July 2010 records for Brown's cell phone numbers must be produced pursuant to Fed. R. Crim. P. 16(a)(1)(E) because they are within the government's possession and are material to his defense (DE 778, at 3-4). Apparently Brown is arguing that the records could be used to show that he was not in the vicinity of the attempted robbery that he is charged with committing on July 26, 2010. In addition, Brown contends that the records are within the government's possession because: (1) NSA is part of the executive branch; (2) the FISA order discussed in the *Guardian* article was obtained pursuant to a Federal Bureau of Investigation ("FBI") affidavit and the FBI is a member of the prosecution team in his case; and (3) the Attorney General's Office, which authorized the government to confer immunity on Davis and decided not to seek the death penalty in this case, is also a member of the prosecution team (DE 778, at 3-4). Alternately, Brown requests that the Court issue a subpoena pursuant to Fed. R. Crim. P. 17, directing the NSA to produce the cell phone records and metadata in its possession relating to Brown's cell phone number for the month of July 2010 (DE 778, at 4).

[5] As of this point in the trial, Brown has not asserted a defense that requires him to admit that he possessed the cell phone at issue on the relevant dates in July 2010.

On June 10, 2013, this Court construed Brown's motion as a request for discovery under 50 U.S.C. § 1806(f), and ordered the government to file a response to Brown's motion and, if it so chooses, an affidavit of the Attorney General of the United States (DE 786). Since the Defendant's filing, the remaining co-defendants have each adopted his Motion as well.

This Court has requested that the Government respond to its Order pursuant to Section 106(f) of the Foreign Intelligence Surveillance Act ("FISA"), codified at 50 U.S.C. § 1806(f). (D.E. 186, at 3-4). Respectfully, the Government submits that Section 1806(f) is not the appropriate vehicle by which to respond to this Court's inquiries because the subject in question does not pertain to information obtained by electronic surveillance, as defined by FISA, but rather to records obtained through the "business records" authority of FISA. However, given the classified nature of the subject at hand, the Government requests that it be permitted to submit a response pursuant to CIPA § 4 and Fed. R. Crim. P. 16, in order to adequately address the Court's concerns.

Section 1806 of Title 50, codifying Section 106 of FISA, establishes procedures relating to the use, suppression, and discovery of information obtained or derived from "electronic surveillance" authorized by either Title I or Title VII of FISA. H.R. Rep. No. 95-1283, at 87 (1978) (noting Section 1806 "places additional constraints on Government use of information obtained *from electronic surveillance* and establishes detailed procedures under which such information may be received in evidence, suppressed, or discovered" (emphasis added)); *see also* 50 U.S.C. § 1881e (extending Section 106's procedural requirements to surveillance conducted pursuant to Sections 702 and 703 of FISA). Section 1806 applies exclusively to information obtained or derived from FISA-

authorized electronic surveillance. Electronic surveillance is itself a term defined in FISA. 50 U.S.C. § 1801(f).

However, the telephony metadata program discussed by the Defendant and in this Court's Order has been publicly confirmed to have been operating pursuant to the non-content "business records" provision (Title V) of FISA, codified in 50 U.S.C. § 1861.[6] While the electronic surveillance provisions contained in Title I of FISA govern the acquisition of communications *(i.e.*, similar to Title III of the Omnibus Crime Control Act of 1968), the business records provision of FISA only provides for the production of "tangible things," analogous to, for example, a grand jury subpoena. 50 U.S.C. § 1861(c)(1) (permitting "the production of a tangible thing if such thing can be obtained with a subpoena *duces tecum*...or with any other order issued by a court of the United States directing the production of records or tangible things"); *see also United States v. Rosen*, 447 F. Supp. 2d 538, 543 n.4 (E.D. Va. 2006) (noting distinction between "electronic surveillance" and "access to business records for foreign intelligence and international terrorism investigations"). Any information obtained pursuant to a business record order would be governed by Title V's own provision governing the use of business-record information, codified in 50 U.S.C. § 1861(h). *See In re NSA Telecommunications Litig.*, 564 F. Supp. 2d 1109, 1126 (N.D. Cal. 2008) (noting different provisions governing use and disclosure in different FISA titles). Section 1861(h), however, does not contain the same procedures as 50 U.S.C. § 1806. Section 1861 lacks a suppression procedure because no defendant would have a reasonable expectation of privacy in business records provided to a third party. The government

[6] This provision is also sometimes known as a "Section 215" order, referring to Section 215 of the USA PATRIOT Act, which established the FISA provision. Pub. L. No. 107-56 § 215, 11 Stat. 272, 287-88 (2001).

therefore feels it is inappropriate to respond to inquiries about business records pursuant to 50 U.S.C. § 1806(f).[7]

At the same time, the Defendant himself acknowledges that any materials he now seeks would relate to a classified program. (D.E. 778, at 2). The Government therefore believes a classified response is necessary to fully brief the Court on this matter. Accordingly, the Government submits this response pursuant to Section 4 of CIPA and Fed. R. Crim. P. 16. Congress passed CIPA in order to "protect against the unauthorized disclosure of classified information in the custody of the federal courts." *United States v. El-Mezain*, 664 F.3d 467, 519 (5th Cir. 2011) (citing *In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 93, 121 (2d Cir. 2008)). CIPA's explicit purpose is to set forth procedures designed to "protect[ ] and restrict[ ] the discovery of classified information in a way that does not impair the defendant's right to a fair trial." *United States v. O'Hara*, 301 F.3d 563, 568 (7th Cir. 2002).

[CLASSIFIED INFORMATION REDACTED]

II. LEGAL STANDARD

A. The Classified Information Procedures Act Governs the Discovery of Classified Information in a Criminal Case

CIPA regulates the use of classified information in criminal proceedings. *United States v. Baptista-Rodriguez*, 17 F.3d 1354, 1363 (11th Cir. 1994).[8] As relevant here,

---

[7] To the extent counsel for the Government has made any reference in court to the Defendant as an "aggrieved party" under FISA, the Government wishes to correct the record and clarify that because the FISC Order relates to the "business records" provision of FISA, and not the "electronic surveillance" provisions of FISA, the Defendant is not and cannot be an aggrieved party as the statute contemplates that term.

[8] CIPA applies to proceedings both before and during trial. *O'Hara*, 301 F.3d at 568 ("CIPA's plain terms evidence Congress' intent to protect classified information from unnecessary disclosure at any stage of a criminal trial.").

CIPA defines "classified information" as "any information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security...." 18 U.S.C. App. 3, § 1(a). "National security" as used in CIPA, "means the national defense and foreign relations of the United States." *Id.*, § 1(b).[9]

"CIPA has no substantive impact on the admissibility or relevance of probative evidence." *United States v. Johnson*, 139 F.3d 1359, 1365 (11th Cir. 1998). *See United States v. Varca*, 896 F.2d 900, 905 (5th Cir. 1990) ("CIPA was not [] intended to expand the traditional rules of criminal discovery under which the government is not required to provide criminal defendants with information that is neither exculpatory nor, in some way, helpful to the defense."). Rather, CIPA "simply ensures that questions of admissibility will be resolved under controlled circumstances calculated to protect against premature and unnecessary disclosure of classified information." *Baptista-Rodriguez*, 17 F.3d at 1364.

[9] Congress enacted CIPA to enable the government to fulfill its duty to protect national security information while at the same time vindicating its interest in prosecuting violations of federal criminal law. *See* S. Rep. No. 96-823 at 3 (1980), *reprinted in* 1980 U.S.C.C.A.N. 4294, 4296. The Act "'was designed to establish procedures to harmonize a defendant's right to obtain and present exculpatory material upon his trial and the government's right to protect classified material in the national interest.'" *United States v. Pappas*, 94 F.3d 795, 799 (2d Cir. 1996) (quoting *United States v. Wilson*, 571 F. Supp. 1422, 1426 (S.D.N.Y. 1983)); *see United States v. Dumeisi*, 424 F.3d 566, 578 (7th Cir. 2005) ("CIPA's fundamental purpose is to 'protect[] and restrict[] the discovery of classified information in a way that does not impair the defendant's right to a fair trial.'") (quoting *O'Hara*, 301 F.3d at 569 (alterations in original)); *United States v. Paracha*, No. 03 CR. 1197(SHS), 2006 WL 12768, at *10 (S.D.N.Y. Jan. 3, 2006) (CIPA "defines by statute a procedure to protect classified information from unnecessary disclosure while at the same time ensuring that a defendant's right to present evidence in his defense is not compromised.") (citations omitted).

B. CIPA Section 4 and Rule 16(d)(1) Permit the Court To Conduct an *Ex Parte, In Camera* Review

Pursuant to CIPA Section 4 and Federal Rule of Criminal Procedure 16(d)(1), the United States is requesting that the Court conduct an *ex parte, in camera* review of the Government's submission. Both CIPA Section 4 and Rule 16(d)(1) expressly authorize the United States to submit an *ex parte* motion seeking an *in camera* review of classified information that may be potentially discoverable in a federal criminal case. CIPA Section 4 provides, *inter alia*:

> The court may permit the United States to make a request for [relief from discovery] in the form of a written statement to be inspected *by the court alone*. If the court enters an order granting relief following such an ex parte showing, the entire text of the statement of the United States shall be sealed and preserved in the records of the court to be made available to the appellate court in the event of an appeal.

18 U.S.C. App. 3, § 4 (1980) (emphasis added). Rule 16(d)(1) contains language that is very similar to that of CIPA Section 4: "The court may permit a party to show good cause [for relief from discovery] by a written statement that the court will inspect *ex parte*. If relief is granted, the court must preserve the entire text of the party statement under seal." Fed. R. Crim. P. 16(d)(1).

Ex parte, in camera proceedings are appropriate to evaluate government claims concerning national security issues. *E.g.*, *United States v. Lee*, 648 F.2d 667, 668 (9th Cir. 1981). Indeed, *ex parte, in camera* consideration of government motions to deny or restrict discovery under CIPA Section 4 consistently has been upheld as a proper practice. *See, e.g.*, *O'Hara*, 301 F.3d at 568 (district court properly conducted *in camera, ex parte* proceeding to determine whether classified information was discoverable); *United States v. Sarkissian*, 841 F.2d 959, 965 (9th Cir. 1988) (*ex parte* proceedings concerning national

security information are appropriate under CIPA Section 4); *United States v. Pringle*, 751 F.2d 419, 427 (1st Cir. 1984) (district court's *in camera*, *ex parte* inspection of potential discovery authorized by Section 4 of CIPA), *vacated and remanded on other grounds sub nom. by United States v. McAfee*, 479 U.S. 805 (1986); *United States v. Marzook*, 435 F. Supp. 2d 708, 745 (N.D. Ill. 2006) ("The plain text of Section 4 specifically permits a court to review classified information *ex parte*.") (citations omitted); *see also United States v. Campa*, 529 F.3d 980, 994-95 (11th Cir. 2008) (district court did not abuse its discretion by holding an *ex parte* hearing under CIPA Section 4); *United States v. Mejia*, 448 F.3d 436, 457-59 (D.C. Cir. 2006) (rejecting defendants' claim of right to participate in CIPA Section 4 hearing).

The rationale for allowing *ex parte* submissions pursuant to CIPA Section 4 is rooted in the purpose of this provision. As the Eleventh Circuit reasoned in *Campa*, "The right that section four confers on the government would be illusory if defense counsel were allowed to participate in section four proceedings because defense counsel would be able to see the information that the government asks the district court to keep from defense counsel's view." *Campa*, 529 F.3d at 995 (citing *Mejia*, 448 F.3d at 457-58; H.R.Rep. No. 96-831, pt. 1, at 27 n.22 (1980)). *See also Sarkissian*, 841 F.2d at 965 (government need not file public claim of privilege before making an *ex parte* submission under CIPA; where "government is seeking to withhold classified information from the defendant, an adversary hearing with defense knowledge would defeat the very purpose of the discovery rules") (quoting H.R. Rep. No. 96-831, at 27 n. 22 (1980)).[10]

[10] CIPA Section 4 requires no particular showing before the Court may grant a request to proceed *ex parte* and *in camera*. *See Sarkissian*, 841 F.2d at 965-66; *Pringle*, 751 F.2d at 427. Rule 16(d)(1), on the other hand, allows *ex parte* proceedings to decide discovery issues on a showing of good cause. *United States v. Hamaker*, 455 F.3d 1316, 1328 n. 11 (11th Cir. 2006) (citing

The provisions for *ex parte* proceedings contained in CIPA Section 4 and Rule 16 are intended to be applied in circumstances such as these, that is, where the government seeks a ruling regarding the discoverability of sensitive classified information.

C. CIPA Section 4 and Rule 16(d)(1) Permit Courts To Restrict Discovery of Classified Information to the Defense

Both CIPA Section 4 and Rule 16(d)(1) authorize a district court to deny or otherwise restrict discovery of classified information by the defense.[11] CIPA Section 4 provides, in pertinent part, that a district court:

> upon a sufficient showing, may authorize the United States to delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure, to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove.

18 U.S.C. App. 3, § 4 (1980). Similarly, Rule 16 of the Federal Rules of Criminal Procedure provides, in pertinent part, that a district court "may, for good cause, deny, restrict, or defer discovery or inspection, or grant other appropriate relief." Fed. R. Crim. P. 16(d)(1).

Fed.R.Crim.P. 16(d)(1)); *see United States v. Nava-Salazar*, 30 F.3d 788, 800-01 (7th Cir. 1994) (government's *ex parte* submissions to district court and court's order delaying discovery authorized and "in full compliance with Rule 16(d)(1)"); *United States v. Pelton*, 578 F.2d 701, 707 (8th Cir. 1978) (*ex parte*, *in camera* proceedings appropriate where prosecutors were concerned about safety of individuals if certain tapes were disclosed to defense); *United States v. Gel Spice Co., Inc.*, 601 F. Supp. 1214, 1219 (E.D.N.Y.1985) (magistrate's *ex parte* review of potential discovery proper under Rule 16(d)(1)).

[11] CIPA's legislative history shows that "Congress intended section 4 to clarify the court's powers under [Rule] 16(d)(1) to deny or restrict discovery in order to protect national security." *Sarkissian*, 841 F.2d at 965 (quoting S. Rep. No. 96-823, at 6 (1980), *reprinted in*, 1980 U.S.C.C.A.N. 4294, 4299-4300). While courts have discretionary authority to consider the need for a protective order in any criminal case, CIPA specifically focuses on how courts should exercise that discretion when classified information is at issue.

Under CIPA Section 4 and Rule 16(d)(1), the Court may authorize the government to withhold from discovery classified materials that are not properly discoverable under the appropriate legal standard. *See United States v. Yunis*, 867 F.2d 617, 624-25 (D.C. Cir. 1989); *United States v. Libby*, 429 F. Supp. 2d 1,7-8 (D.D.C. March 10, 2006).

D. CIPA Section 4 and Rule 16(d)(1) Permit Courts To Withhold Classified Information From the Defense Where the Evidence Is Not at Least Relevant and Helpful

In determining whether to authorize the government to withhold classified materials from discovery under CIPA Section 4 or Rule 16(d)(1), courts apply a classified national security information privilege that protects against the information's disclosure on a "mere showing of theoretical relevance." *Yunis*, 867 F.2d at 623. This privilege is based on the indisputable importance of protecting the nation's secrets from disclosure. *Id.* at 622-23; *see also CIA v. Sims*, 471 U.S. 159, 175 (1985); *Chicago & Southern Air Lines, Inc. v. Waterman S. S. Corp.*, 333 U.S. 103, 111 (1948).

In assessing the government's discovery obligations under Rule 16 and the Constitution concerning material covered by the classified information privilege, courts have applied the government informant's privilege test set forth in *United States v. Roviaro*, 353 U.S. 53 (1957). *See Yunis*, 867 F.2d at 623. Notably, judicial recognition of a "national security" or "classified information" privilege predates CIPA's enactment in 1980, *see United States v. Nixon*, 418 U.S. 683, 705-07 (1974); *Chicago & Southern Air Lines, Inc.*, 333 U.S. at 111, as does the *Roviaro* informant's privilege.

In *Roviaro*, the United States Supreme Court considered application of the informant's privilege – pursuant to which the government may withhold from disclosure

the identity of its informants – to the general rules of discovery in a criminal case. *Roviaro*, 353 U.S. at 59. The Court noted that the privilege implicates two fundamental, competing interests: (1) the interest of the defendant in mounting a defense; and (2) the public interest in enabling the government to protect its sources. *Id.* at 59-61. The Court first described a fairness principle that had been applied by the Courts of Appeal: "Where the disclosure of an informer's identity, or of the contents of his communication, is relevant and helpful to the defense of an accused, or is essential to a fair determination of the cause, the [informer's] privilege must give way." *Id.* at 60-61. But then the Court held that "no fixed rule with respect to disclosure is justifiable," and that "the problem is one that calls for balancing the public interest in protecting the flow of information against the individual's right to prepare his defense." *Id.* at 62. The Court held that the result of such balancing "must depend on the particular circumstances of each case, taking into consideration the crime charged, the possible defenses, the possible significance of the informer's testimony, and other relevant factors." *Id.*

In *Yunis*, the Court of Appeals for the District of Columbia Circuit applied *Roviaro's* reasoning in interpreting CIPA's statutory requirements, holding that classified information may be withheld from discovery if it is not both relevant and "at least 'helpful to the defense of [the] accused.'" *Yunis*, 867 F.2d at 623 (quoting *Roviaro*, 353 U.S. at 60-61) (alteration in original).

Where a defendant seeks to compel disclosure of classified information, he must show more than "theoretical relevance in the face of the government's classified information privilege." *Id.* at 623. Rather, to overcome this privilege, the defense "is

entitled only to information that is at least 'helpful to the defense of [the] accused,"[12] *Id.* (quoting *Roviaro*, 353 U.S. at 60-61) (alterations in original),[13] or "essential to the fair resolution of the cause." *Yunis*, 867 F.2d at 625.

Courts considering issues under CIPA Section 4 and Rule 16(d)(1) have applied the "relevant and helpful" standard in assessing the discovery of classified information. *See, e.g., Mejia*, 448 F.3d at 455-57; *United States v. Varca*, 896 F.2d 900, 905 (5th Cir.1990); *Pringle*, 751 F.2d at 427-28 (upholding district's court exclusion of classified evidence that "'was not relevant to the determination of the guilt or innocence of the defendants, was not helpful to the defense and was not essential to a fair determination of the cause'") (quoting district court's opinion) (citing *Brady*, 373 U.S. 83; *Roviaro*, 353 U.S. 53); *Paracha*, 2006 WL 12768 at *9; *United States v. Rahman*, 870 F. Supp. 47, 50 (S.D.N.Y. 1994). A court applying this standard should "err on the side of protecting the interests of the defendant." *United States v. Rezaq*, 134 F.3d 1121, 1142 (D.C. Cir. 1998); *see Rahman*, 870 F. Supp. at 51 (court reviewed classified information as potentially discoverable "in the light most favorable to defendants").

III. ARGUMENT

The Defendant has moved the Court to order the government to produce "the records for the two telephones that [the Government] attributes to [the Defendant] for the dates which are relevant to this case—the month of July 2010." (DE 778) As discussed

---

[12] Exculpatory or impeachment information discoverable under *Brady*, *Giglio*, and their progeny are subsumed within the category of information that is "at least helpful" to the defense. *See Mejia*, 448 F.3d at 456-57.

[13] If the Court does not find the defense is entitled to discovery of this information under *Roviaro*, then the defense would not have a "need-to-know." Executive Order 13526 Section 4.1 sets forth the requirements for access to classified information and states that before such access is given, all persons must be cleared by the appropriate agency head or designee, and have a need-to-know. Exec. Order No. 13526 Section 4.1(a)(1) & (3), 73 Fed. Reg. 128 (July 2, 2008).

in greater detail above, the defendant incorrectly believes that the Government is in possession of these records based on illegally leaked classified information in a June 5, 2013 *Guardian* newspaper article, which published a classified FISA Court order appearing to grant the NSA authority to collect telephony metadata from Verizon. The Defendant claims that the Government, pursuant to the terms of this leaked FISA Court order, may possess metadata, particularly CSLI, from calls made in July 2010 from the Defendant's cellular telephone numbers. Because the Defendant believes that this metadata may be exculpatory, in that it would show that he was not physically located at the scene of the alleged robbery in July 2010, he argues that due process requires the production of these alleged records pursuant to *Brady v. Maryland*, 373 U.S. 83 (1963), as exculpatory evidence, and Rule 16, as documents or data "material to preparing the defense."[14] Fed. R. Crim. P. 16(a)(1)(E)(i). The Defendant further requests, to the extent the Court finds the records are not in the possession of the prosecution team, that the Court issue a Rule 17 subpoena to the NSA to obtain the records.

At the outset, the government does not possess the CSLI data that the Defendant seeks. As explained above, the program described in the classified FISA order cited by the defense did not acquire such data.

[CLASSIFIED INFORMATION REDACTED]

[14] "Material" as used in the phrase "material to the preparation of the defense" in Rule 16(a)(1)(E)(i), and "helpful to the defense," as used in the *Yunis/Roviaro* line of cases discussed above, may be essentially the same standard. *See Yunis*, 867 F.2d at 625 (noting that "relevant and helpful" standard was not new test but concluding that it provided better guidance than term "materiality," which also was used in *Roviaro*). In any event, the Government submits that the information and documents discussed below as not being "helpful" to the defense also are not "material" to the defense, as defined by Rule 16(a)(1)(E)(i).

B. Neither Brady Nor Rule 16 Permit the Defendant to Conduct a Fishing Expedition of Highly Classified NSA Data

[CLASSIFIED INFORMATION REDACTED]

Pursuant to *Brady v. Maryland*, 373 U.S. 83 (1963) and its progeny, the Government must provide to the Defense, in time for effective use at trial, any evidence favorable to the accused that is material to guilt or punishment. Evidence is material "if there is a reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different." *Youngblood v. West Virginia*, 547 U.S. 867, 870 (2006) (per curiam) (citations omitted). In other words, there must be a "showing that the favorable evidence could reasonably be taken to put the whole case in such a different light as to undermine confidence in the verdict." *Id.* (quoting *Kyles v. Whitley*, 514 U.S. 419, 435 (1995)). In *Kyles*, the Supreme Court held that, in analyzing materiality, the touchstone inquiry is whether, in the absence of the evidence at issue, the defendant could receive a fair trial, that is, a trial resulting in a "verdict worthy of confidence." *Kyles*, 514 U.S. at 434.

The obligation to provide the *Brady* information exists, without a specific request, when the evidence is of obvious substantial value to the defense. *See Grossman v. McDonough*, 466 F.3d 1325, 1341-42 (11th Cir. 2006). The Government has no obligation, however, to produce information that it does not possess or of which it is unaware. *See Halliwell v. Strickland*, 747 F.2d 607, 609-10 (11th Cir. 1984).

Rule 16(a)(1) of the Federal Rules of Criminal Procedure identifies specific categories of information or materials that are "subject to disclosure" after a defendant's request. The category of Rule 16 evidence at issue in this motion comprises items that may be subject to disclosure under Rule 16(a)(1)(E)(i), that is, documents or objects in

the government's possession that are material to the preparation of the defense. In this context, the "defense" "means the defendant's response to the Government's case-in-chief." *United States v. Armstrong*, 517 U.S. 456, 462 (1996). To meet the materiality standard of Rule 16(a)(1)(E), a "defendant must 'show' 'more than that the [item] bears some abstract logical relationship to the issues in the case.... There must be some indication that the pretrial disclosure of the [item] would ... enable [] the defendant significantly to alter the quantum of proof in his favor." *Jordan*, 316 F.3d at 1251 (quoting *United States v. Buckley*, 586 F.2d 498, 506 (5th Cir. 1978)) (other citation omitted) (alterations in original); *see also United States v. Lloyd*, 992 F.2d 348, 350-51 (D.C. Cir. 1993); *United States v. Reeves*, 892 F.2d 1223, 1226 (5th Cir. 1990). Neither the Defendant nor his co-defendants can meet this burden here.

C. The Information at Issue Is Highly Classified and Subject to a National Security Privilege and Should Be Protected from Disclosure

Because CIPA governs the handling of classified information, any motion under CIPA must establish that the information at issue is indeed classified and subject to a claim of privilege.[15] *Mejia*, 448 F.3d at 455; *Sarkissian*, 841 F.2d at 966. The Government has a "'compelling interest' in withholding national security information from unauthorized persons in the course of executive business." *Dep't of Navy v. Egan*,

---

[15] As noted above, "classified information," as used in CIPA, includes "any information or material that has been determined by the United States Government pursuant to an Executive order, statute or regulation, to require protection against unauthorized disclosure for reasons of national security." 18 U.S.C. App. III § 1(a). "National security" means the national defense and foreign relations of the United States. *Id.* at § 1(b). In order to establish these facts, the Government ordinarily submits a declaration or affidavit executed by an official with classification review authority. Such a declaration, *inter alia*: "(1) describes the reasons for the classification of the information at issue; and (2) sets forth the potential harm to national security that could result from its disclosure." *United States v. Libby*, 429 F. Supp. 2d 18, 25 (D.D.C. 2006)(citation omitted); *see also Rahman*, 870 F. Supp. at 50. Thus the Government has such a Declaration with this memorandum.

484 U.S. 518, 527 (1988) (quoting *Snepp v. United States*, 444 U.S. 507, 509 n.3 (1980)). As the Supreme Court repeatedly has stressed, courts are "reluctant to intrude upon the authority of the Executive in . . . national security affairs." *Egan*, 484 U.S. at 530 (additional citations omitted); *see Ctr. for Nat'l Sec. Studies v. U.S. Dept. of Justice*, 331 F.3d 918, 926-27 (D.C. Cir. 2003). Accordingly, courts have recognized that the determination of whether to classify information and the proper classification thereof is a matter committed solely to the Executive Branch: "[T]he government ... may determine what information is classified. A defendant cannot challenge this classification. A court cannot question it." *United States v. Smith*, 750 F.2d 1215,1217 (4th Cir. 1984); *see United States v. Musa*, 833 F. Supp. 752, 755 (E.D. Mo. 1993).

[CLASSIFIED INFORMATION REDACTED]

IV. CONCLUSION

Based on the foregoing, pursuant to CIPA Section 4 and Rule 16(d)(1) of the Federal Rules of Criminal Procedure, the Government respectfully requests that the Court: (1) conduct an *in camera* and *ex parte* review of the Government's submission; (2) deny the Defendant's Motion to Compel Production of Phone Records and request for a Rule 17 subpoena to obtain the records, because the Government has no reason to believe that responsive records exist under *Brady v. Maryland*, 373 U.S. 83 (1963), and Fed. R. Crim. P. 16; (3) find that to the extent any records existed, they should be deleted from discovery under CIPA Section 4; (4) strike the Defendant's Notice under Section 5 of CIPA; and (5) order that the entire text of this motion, all accompanying exhibits and any

classified order issued by the Court shall not be disclosed to the defendants and shall be sealed and preserved in the records of the Court to be made available to the appellate court in the event of an appeal.

Respectfully submitted,

WILFREDO A. FERRER
UNITED STATES ATTORNEY

/s/ Brian K. Frazier
Brian K. Frazier
Assistant United States Attorney
Court No. A5500476
U. S. Attorney's Office
99 N.E. 4th Street
Miami, FL 33132
Tel: (305) 961-9009
Fax: (305) 536-4675

Michael J. Mullaney
Chief, Counterterrorism Section
National Security Division
Florida Bar No.0794317
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of Court using CM/ECF on this the 19th day of June 2013.

/s/ Brian K. Frazier
Brian K. Frazier